Notice of Allowability	Application No.	Applicant(s)	
	10/769,103	BODORIN ET AL.	
	Examiner	Art Unit	
	TESHOME HAILU	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *04/17/2009*.

2. ☒ The allowed claim(s) is/are *1, 4 and 7-24*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20090703* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☒ Other *See examiner comments.*.

DETAILED ACTION

1. In an amendment filed on April 17, 2009, claims 1, 4 and 7-24 have been amended.

2. Claims 1, 4 and 7-24 are pending.

Response to Arguments

3. Applicant's arguments filed on April 17, 2009, with respect to the rejection of claims 1, 4 and 7-24 have been fully considered in view of the amended claims and are persuasive. The rejections of claims 1, 4 and 7-24 have been withdrawn.

Allowable Subject Matter

4. Claims 1, 4 and 7-24 are allowed. No reason for allowance is needed as the record is clear in light of applicant's arguments and specification.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicant representative, Jens Jenkins (Reg. No. 44,803), on July 3, 2009. The following amendment to the claims will replace the previous set of claims.

1. (Currently Amended) A computer implemented system for determining whether a packed executable is malware, the system comprising:

A processor;

a malware evaluator for determining whether incoming data is malware, wherein the incoming data directed to a computing device is intercepted by the malware evaluator; and

an unpacking module that receives a first packed executable from the malware evaluator and returns ~~an~~ a corresponding substitute unpacked executable, without executing the first packed executable during unpacking, ~~corresponding to the entire packed executable;~~ the unpacking module comprising:

at least one substitute unpacker code segment, corresponding to a first unpacker code segment of the first packed executable, such that an appropriate substitute unpacker code segment is substituted for the first unpacker code segment of the received first packed executable to facilitate unpacking the first packed executable according to the substitute unpacker code rather than according to the first unpacker code, the first packed executable is thereby unpacked into a corresponding substitute unpacked executable that can be the same as, or different than, a first unpacked executable unpacked if the first packed executable were unpacked by the first unpacker code;

an unpacking manager, wherein the unpacking manager, upon obtaining the first packed executable, selects the unpacking module for a set of unpacking module to unpack the first packed executable according to a type of the first packed executable, and executes the selected unpacking module which generates the first unpacked executable corresponding to the first packed executable.

wherein the malware evaluator, upon receiving incoming data, can at least in part determine whether the incoming data is a packed executable, and if so, the malware evaluator provides the packed executable to the unpacking module such that ~~an~~ a substitute unpacked executable, corresponding to the first packed executable, is generated by unpacking the first packed executable with a substitute unpacker code segment without executing the first packed executable, whereby ~~can be received from the unpacking module, such that~~ the malware evaluator can determine whether the first unpacked executable ~~is~~ would be malware based at least in part on an analysis of the corresponding substitute unpacked executable.

2. (Cancelled)

3. (Cancelled)

4. (Currently Amended) A computer-implemented method for determining whether incoming data is malware, wherein the method is implemented by a computing device having a processor, the method comprising:

intercepting incoming data directed to the computing device having a processor;

determining whether the incoming data is a packed executable; and if the incoming data is a packed executable:

accessing at least one substitute unpacker code segment corresponding to a first incoming packed executable of the incoming data;

substituting the substitute unpacker code segment for a first unpacker code segment of the first packed executable;

generating ~~an~~ a substitute unpacked executable employing the substitute unpacker code segment, the substitute unpacked executable corresponding to ~~the entire~~ a first unpacked ~~packed~~ executable that would result from unpacking the first packed executable with the first unpacker code; and

determining whether the first incoming packed executable is malware by evaluating whether the corresponding substitute unpacked executable ~~is~~ includes malware.

5. (Cancelled)

6. (Cancelled)

7. (Currently amended) The system of Claim 1, wherein the returned substitute unpacked executable corresponding to the packed first executable is based at least in part on code or data derived from employing ~~an~~ the substitute unpacker code rather ~~other~~ than the loader/unpacker received with the first packed executable.

8. (Currently amended) The system of Claim 7, wherein the employed substitute unpacker code is selected from a group of at least one modularized substitute unpacker modules germane to unpacking a first packed executable of a particular type and further germane to unpacking a first packed executable that has been intercepted by the malware evaluator.

9. (Previously Presented) The system of Claim 1, wherein the intercepted incoming data resides only in one or more logically or physically isolated memory stores such that the intercepted incoming data can be located at a computer but does not actually "reach" the computer.

10. (Previously Presented) The system of Claim 9, wherein the one or more isolated memory stores comprise at least one of a floppy disk, a flash memory storage device, magnetic tape, or combinations thereof.

11. (Currently amended) The system of Claim 1, wherein the corresponding substitute unpacked executable generated by the unpacking module corresponds to a complete first packed executable and not just a portion thereof.

12. (Currently amended) The system of Claim 11, wherein the corresponding generated substitute unpacked executable corresponding to a complete unpacked executable is unpacked without executing any portion thereof.

13. (Previously Presented) The system of Claim 1, wherein the malware evaluator determines whether the incoming data is malware without unpacking the incoming data if the incoming data is determined not to be a packed executable.

14. (Currently Amended) The system of Claim 1, wherein the incoming data can be intercepted from at least one data source including a computer network, ~~and~~ or distributable media further including a floppy disk, a flash memory storage device, a CD-ROM disk, a magnetic tape, or combinations thereof.

15. (Previously Presented) The system of Claim 1, further comprising, first determining whether the incoming data is known malware before determining if the incoming data is a packed executable, and if not, then determining if the incoming data is a packed executable.

16. (Previously Presented) The system of Claim 15, wherein anti-virus software can be employed in determining whether the incoming data is malware.

17. (Previously Presented) The system of Claim 16, wherein the determining by anti-virus software can be by signature or pattern recognition processes.

18. (Previously Presented) An electronic device comprising the system of Claim 1, such that the electronic device can be placed between a network and a computer device to facilitate intercepting data directed to a computing device.

19. (Previously Presented) The method of Claim 4, further comprising, first determining whether the incoming data is known malware before determining if the incoming data is a packed executable.

20. (Currently amended) The method of Claim 4, wherein generating ~~an~~ a corresponding substitute unpacked executable at least in part employs ~~an~~ a substitute unpacker code segment other than the loader/unpacker received with the first packed executable.

21. (Currently amended) The method of Claim 20, wherein the employed substitute unpacker code is selected from a group of at least one modularized substitute unpacker modules germane to unpacking a

first packed executable of a particular type and further germane to unpacking a first packed executable that has been intercepted.

22. (Previously Presented) The method of Claim 4, wherein intercepting incoming data intercepts data as it arrives at the computing device from a network or a distributable media.

23. (Currently amended) The method of Claim 4, wherein generating the corresponding substitute unpacked executable occurs without executing any portion of the unpacked executable.

24. (Currently amended) The method of Claim 4, wherein the corresponding unpacked executable corresponds to a complete first packed executable and not just a portion thereof.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Teshome Hailu/

Examiner, Art Unit 2434

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434